What is claimed is:

1 - A computer network comprising:

a local computer;

a userid associated with a user of the local computer, said userid having a secret password associated therewith;

a host computer;

a communications mechanism connecting the host computer to the local computer wherein the local computer requests access to the host computer by:

sending the userid and a first nonce to the host computer;

the host computer responds to the local computer by sending a second nonce to the local computer;

the local computer then sends the host computer an authentication token comprising a hashed value of the combination of the userid and password, the first nonce and the second nonce;

the server verifies the hashed value using copies of the authentication token, first nonce and second nonce residing at the host computer;

the host computer allows the user at the local computer to access information at the host computer only if the verification is successful.

2- A computer network comprising:

a local computer;

a userid associated with a user of the local computer; said userid having an original password associated therewith;

a host computer; and,

a communications mechanism connecting the host computer to the local computer wherein the local computer accesses the host computer by using the original password and wherein the local computer changes the original password for accessing the host computer to a new password by sending a first random value and the userid of the user to the host computer, the host computer generates a second random value

and sends it to the local computer, the local computer generates an authentication token using a hash function, the userid, the original password and a digest of the new password and sends the authentication token and the digest to the host computer, wherein the host computer accepts the change of the password to the new password if the host computer can verify the authentication token.

3 - A network as claimed in claim 2 wherein the host computer verifies the authentication token using a copy of the first random value, a copy of the second random value and a copy of the authentication token residing at the host computer.

4- A network as claimed in claim 2 wherein said hash function is a collision-resistant, one-way hash.

5 - A method for accessing information on a host computer by a local computer over a network, the local computer having a user and a user identifier (userid) associated therewith, the userid also having a password associated therewith, the method comprising the steps of:

sending, by the local computer, a message across the network to the host computer, the message comprising the userid of the user at the local computer and a first nonce;

replying, by the host computer to the local computer, by sending a reply across the network, the reply comprising a second nonce;

creating, by the local computer, a userid-password digest using a hash function on the userid and the password;

calculating, by the local computer, an authentication token, the authentication token comprising a hashed value of the userid-password digest, the first nonce and the second nonce;

transmitting, by the local computer to the host computer, the userid and the authentication token;

verifying, by the host computer, that the authentication token is valid for the userid, the host computer using copies of the first nonce, the second nonce and the userid-password digest stored at the host computer;

allowing the user at the local computer to access information at the host computer only if the verification step is successful.

6. A method for securely changing an existing password associated with a user identifier (userid) on a host computer to a new password, wherein said passwords enable a user associated with said userid at a local computer to access information on said host computer across a network; said method comprising the steps of:

sending, by the local computer, the userid and a first nonce to the host computer;

replying, by the host computer to the local computer, with a second nonce;

generating, by the local computer, a first digest of the userid and the existing password and a second digest of the userid and the new password;

creating, by the local computer, an authentication token and an authentication token mask wherein said authentication token si a hash function of the first digest, first nonce and second nonce, and said token mask is a hash function of the second digest, first nonce plus a predetermined value and the second nonce;

generating, by the local computer, a protected digest by exclusive-or'ing the second digest with the token mask;

sending, by the local computer to the host computer, the userid, authentication token and the protected digest;

verifying, by the host computer, the validity of the authentication token; and,

accepting the new password to replace the existing password if the authentication token is valid.

7. A method as claimed in claim 5 wherein said first and second digests are calculated by performing a hash function on the userids and respective passwords.

8. A method as claimed in claim 5 or 6 wherein said hash function is a collision-resistant, one-way hash.

9 - A computer program product for accessing information on a host computer by a local computer over a network, the local computer having a user and a user identifier (userid) associated therewith, the userid also having a password associated therewith, the method comprising:

computer readable programming means for sending, by the local computer, a message across the network to the host computer, the message comprising the userid of the user at the local computer and a first nonce;

computer readable programming means for replying, by the host computer to the local computer, by sending a reply across the network, the reply comprising a second nonce;

computer readable programming means for creating, by the local computer, a userid-password digest using a hash function on the userid and the password;

computer readable programming means for calculating, by the local computer, an authentication token, the authentication token comprising a hashed value of the userid-password digest, the first nonce and the second nonce;

computer readable programming means for transmitting, by the local computer to the host computer, the userid and the authentication token;

computer readable programming means for verifying, by the host computer, that the authentication token is valid for the userid, the host computer using copies of the first nonce, the second nonce and the userid-password digest stored at the host computer;

computer readable programmnig means for allowing the user at the local computer to access information at the host computer only if the verification step is successful.

10. A computer program product for securely changing an existing password associated with a user identifier (userid) on a host computer to a new password, wherein said passwords enable a user associated with said userid at a local computer to access information on said host computer across a network; said method comprising the steps of:

computer readable programming means for sending, by the local computer, the userid and a first nonce to the host computer;

computer readable programming means for replying, by the host computer to the local computer, with a second nonce;

computer readable programming means for generating, by the local computer, a first digest of the userid and the existing password and a second digest of the userid and the new password;

computer readable programming means for creating, by the local computer, an authentication token and an authentication token mask wherein said authentication token is a hash function of the first digest, first nonce and second nonce, and said token mask is a hash function of the second digest, first nonce plus a predetermined value and the second nonce;

computer readable programming means for generating, by the local computer, a protected digest by exclusive-or'ing the second digest with the token mask;

computer readable programming means for sending, by the local computer to the host computer, the userid, authentication token and the protected digest;

computer readable programming means for verifying, by the host computer, the validity of the authentication token; and,

computer readable programming means for accepting the new password to replace the existing password if the authentication token is valid.

11. A computer program product as claimed in claim 10 wherein said first and second digests are calculated by performing a hash function the userids and respective passwords.

12. A computer program product as claimed in claim 10 or 11 wherein said hash function is a collision-resistent, one-way hash.